Accellion

AN ACCELLION WHITE PAPER

Best Practices for Implementing Enterprise Secure File Transfer

SECURE, COMPLIANT, EASY TO USE, AND EASY TO MANAGE

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485 4300
Fax +1 650 485 4308
www.accellion.com
info@accellion.com

Executive Summary

Every type of organization needs to protect confidential information, whether for regulatory compliance or simply for economic competitiveness. Security breaches that expose confidential data are dangerous and costly. The results can include regulatory penalties, civil lawsuits, and lost business.

Security breaches that expose confidential information are costly and yet enterprises still do a poor job of protecting data in transit.

To avoid these breaches, enterprises need data security. By now, most enterprises have effective measures for protecting data at rest in databases and archived storage systems. But enterprises still do a poor job of protecting data in transit. They rely on unsecure tools, such as FTP or instant messaging, for transferring files from one location to another. They allow confidential data to accumulate on untended FTP servers or to leak out through P2P or email. To correct these problems, enterprise IT departments sometimes impose overly rigid security procedures on users. Users then revert to using unsecure channels and risky workarounds so they can get data transfers over and done with.

Enterprises need a secure file transfer solution that enables authorized users to transfer files quickly, easily, and securely to other authorized users—all within a system managed and monitored by IT.

.

Enterprise Data at Risk

Protecting information assets is a top priority for all enterprises. Every type of organization has data it needs to protect. The data might be confidential intellectual property, financial data, customer records, or industry-specific data such as patient health information.

Considering the importance of keeping data secure, it is surprising that so many enterprises continue to put themselves at risk for data breaches.

When information assets are exposed through a data breach, the results are costly. Data breaches that violate laws such as Sarbanes-Oxley, industry regulations such as HIPAA (Health Insurance Portability and Accountability Act), and those mandated by FINRA can result in steep financial penalties. A growing number of state and federal laws require organizations to notify the public of data breaches. When the public learns that a company has lost or mishandled sensitive data, the company's reputation and brand value can suffer. Data breaches can lead to a loss of trust and to customer defections. In many cases, lost data results in lost business. Data breaches may also give competitors access to valuable information or hackers access to confidential data they can exploit for financial gain.

Considering the importance of keeping data secure, it is surprising that so many enterprises continue to put themselves at risk for data breaches. Enterprises may guard their internal data with sophisticated firewalls, secure databases, and rigorous IT processes, but when it comes to transferring confidential data from one location to another, too often enterprises are asleep at the wheel. They rely on outdated, unsecure file transfer tools. Or they impose such rigid procedures on employees and partners that users find unsecure alternatives for transferring files.

What IT departments fail to do is provide secure, manageable tools that are so easy-to-use that users are never tempted to find workarounds. When file transfer is secure, manageable, and easy to use, employees and partners will use the system that IT provides. Then file transfer becomes a secure, manageable IT practice, rather than an unsecured IT risk.

What are the common unsecure file transfer tools that put enterprise data at risk?

- FTP, which tempts users to upload confidential files on servers and then forget about them.
- P2P, which relies on client configurations with default settings that often broadcast all sorts of confidential data onto the Internet.
- IM, which often transfers files without encryption and which makes it easy to spoof recipients' IDs.
- Courier services, which can lead to physical media such as tapes and CDs being lost or mishandled.
- Free file-sharing services, which IT is unable to administer and which may leak data to untrusted third parties.
- USB memory sticks, which can be lost or stolen, and which make data untraceable by IT.

When enterprises try to compensate for these unsecured file transfer methods by imposing draconian procedures on users, users find alternatives. They sign up for online file-sharing services. Or they mail USB sticks and CDs. Or they take advantage of Gmail's generous size restrictions and email confidential data to users. One way or another, users will find a way to transfer files quickly and easily, so they can get on with the rest of their work.

As a result of these unsecure tools and end-user workarounds, the enterprise loses control of its data security. The IT department has no way of ensuring that confidential data is protected, because that data is scattered across dozens of FTP servers and file-sharing services, or, worse, it's scattered across tens or hundreds of thousands of P2P nodes around the world. Users never notice the data breaches that are taking place on their desktops and servers day after day. Whether the enterprise realizes it or not, it faces growing risks in the areas of regulatory compliance penalties, customer defections, and litigation. Eventually, a bad data breach occurs. And the enterprise must face the consequences.

There is an easy way to greatly reduce the risk of data breaches while removing the temptation for users to circumvent IT security measures. Enterprises can implement an enterprise-wide secure file transfer solution.

The Solution: Secure File Transfer

There is an easy way to greatly reduce the risk of data breaches while removing the temptation for users to circumvent IT security measures. Enterprises can implement an enterprise-wide secure file transfer solution that's easy to use, easy to integrate, and easy to manage.

A secure file transfer solution enables users to send files securely to trusted users without relying on FTP, data sticks, or other unsecured methods. The solution transfers files securely over channels that can be monitored and managed by the IT department. Reporting tools confirm which files have been received, who accessed them, and when. The best solution supports two-way communication among all authorized users, including partners and trusted users outside the enterprise. Employees are not tempted to abandon the secure solution as soon as they need to transfer files to a recipient who might not already have an account. The solution enables secure communication with the enterprise's community of business users, adapting as that community grows and evolves.

By adopting a secure file transfer solution and abandoning risky file-sharing practices, an enterprise can better protect its confidential data and simplify compliance with industry regulations and federal data-security laws.

Best Practices for Implementing Secure File Transfer

Like any technology introduced to a community of users, secure file transfer solutions can be implemented in various ways, impose various demands, and achieve varying levels of success.

Here's a list of best practices for implementing a secure file transfer solution in an enterprise:

1. Ensure ease of use and transparency to users

Implement a solution that fits into the software tools and business processes that employees use every day. Make secure file transfer so transparent and easy that employees are no longer tempted to use alternatives, such as private file transfer accounts and Gmail. Best-of-breed solutions can be integrated to work with email systems, Web browsers, and other applications that employees use every day.

2. Disable FTP and delete old files stored on FTP servers.

While ostensibly secure, FTP leads to many file security problems. Some problems arise because FTP is often cumbersome to administer and manage. To use FTP securely, users need unique, password-protected accounts. Setting up such accounts falls to IT managers who often have higher priority issues. As a result, getting an account set up can take time—sometimes days or weeks, if IT is backed up. In the meantime, business waits. The delay prompts users to seek alternatives. Why wait for a special FTP account when you can send the file immediately with Gmail or post it on a free file-sharing site like drop.io?

When employees do use FTP, other problems result. Files linger on servers because once the recipient has the file, the sender has little incentive to log onto the server and delete it. As a result, FTP servers become repositories for old, untended confidential files. Clogged servers become targets for hackers. And unscrupulous FTP users may pore through directories, looking for interesting data.

3. Block P2P programs and warn employees about the dangers of P2P.

A couple of years ago, a major pharmaceutical company inadvertently leaked confidential data about 17,000 employees onto the Internet. The data included Social Security numbers. What caused the leak? An employee's spouse had installed P2P software on a company laptop. The software's default configuration generously shared the contents of the laptop's hard drive with the public. Another employee sued, and Connecticut's attorney general launched an investigation. P2P clients are among the most popular software downloads, but few users realize just how risky P2P file-sharing really is. The default configurations of many P2P clients broadcast data from local hard drives. Users are often too swept up with their new music or movies to notice.

4. Extend secure file transfer capabilities to IM.

Millions of employees already communicate quickly and casually over IM every day. They often transfer files using IM as well, with little or no security controls such as encryption, authentication, or reporting. The problem of users transferring files unsecured over IM is only going to get worse. Gartner predicts that 95% of employees will use IM as their primary tool for voice, video, and text chat communications by 2013.

By integrating the secure file transfer solution with IM clients, enterprises can achieve two important goals. First, they can ensure that file transfers over IM are secure and well-managed. Second, they can ensure that the secure file transfer solution remains the sole platform and repository of record that users trust for transferring files, regardless of the client technology being used: Web browser, email client, or even IM.

5. Protect files in transit.

Protect files in transit with SSL, data encryption, and password authentication.

6. Protect files at rest.

Protect files at rest with data and disk encryption and password authentication.

7. Let authorized users help themselves.

Enable business partners and other trusted outsiders to easily gain access and use the same secure file transfer system for sending and receiving files securely. Eliminate the need for IT managers to manually create accounts before files can be transferred.

8. Set policies that limit the sharing of confidential information via courier services.

In July 2010, FedEx lost 138,000 patient health records when it was shipping CDs for a New York City hospital. In 2009, FedEx delivered 8,500 confidential W-2 forms to the wrong addresses.

There are some situations that require paper originals and the use of courier services. But in many cases, sending files electronically is faster safer, and more secure. Another benefit of using digital file transfer is that it consumes much less energy and results in much less pollution. A secure file transfer solution is "greener" than courier services relying on airplanes and trucks.

9. Audit file transfers to ensure best practices and industry regulations are being met.

Once the secure file solution is deployed, IT manager and security officers should communicate updated secure file transfer best practices. Then they should audit the solution's use to ensure that users have genuinely changed their habits and are transferring files securely. By monitoring file traffic and account activity, while keeping an eye on the use of courier services, Gmail, and other communication channels, IT and security personnel can gain an understanding of which users and departments might be clinging to their old habits and putting data security and regulatory compliance at risk.

10. Educate employees and include secure file transfer policies in overall security guidelines.

Educating users is an essential step for IT security. Enterprises should document their file transfer policies, explain the risks of applications such as P2P and IM, and train users on using the secure file transfer solution.

Once users recognize the risks of unsecured and unauthorized file-sharing methods and understand the capabilities of the secure file transfer solution at their fingertips, they are less inclined to resort to using alternatives. It will also enable the IT departments to more quickly and thoroughly meet the demands of compliance officers and regulators.

The Accellion Secure File Transfer Solution

Accellion provides enterprise-class managed file transfer solutions for security and data leak prevention that meet today's business requirements for digital information transfer. The world's leading corporations and government agencies rely on Accellion Secure File Transfer to secure their intellectual property and ensure compliance. Designed with unparalleled flexibility and scalability, Accellion provides organizations with flexible deployment options that can grow from a single office to global distributed deployment integrating virtual, public and private cloud installations.

With Accellion Secure File Transfer, organizations can protect the transfer of intellectual property, reduce security exposure, ensure compliance, improve email performance, replace non-secure FTP and reduce IT support, all while providing business users with a file transfer solution that works for them.

Accellion has a global customer base spanning multiple industries including healthcare, pharmaceutical, financial, legal, government, advertising, education, industrial, entertainment and media. Accellion customers include Procter & Gamble; Activision; Clarian Health Partners; Kaiser Permanente; Foley & Mansfield; Lovells; Bridgestone; Ogilvy & Mather; Harvard University; Guinness World Records; US Securities and Exchange Commission; and NASA.

KEY BENEFITS

- Ensures end-to-end file transfer security
- Enables transfer of large files up to 50GB in size
- Provides comprehensive file tracking for SOX, HIPAA, and GLBA compliance
- Eliminates FTP security and support issues
- Addresses email attachment size limits
- Reduces email storage requirements
- Provides easy account management
- Automates file lifecycle management

.

About Accellion

Founded in 1999, Accellion, Inc. is the premier provider of on-demand secure file transfer solutions with an extensive customer base covering industries such as advertising/media production, legal, manufacturing, healthcare, consumer goods, higher education, and more.

Accellion provides an enterprise file transfer solution that is secure, economical and easy to use for both end users and IT management. Unlike email and FTP that can no longer meet the evolving security and business requirements, Accellion enables enterprises to eliminate FTP servers, create Sarbanes-Oxley compliant business processes, improve email infrastructure performance, and reduce IT management footprint requirements.

The Accellion secure file transfer solution allows internal and external users to send and receive files bi-directionally on the same platform without adding administrative overhead or infrastructure burden. Accellion offers an intuitive web interface with end-to-end file security and policy-based file lifecycle management. Accellion also supports plug-in integration with Outlook and Lotus Notes email clients and for Microsoft SharePoint and OCS applications. For multi-site enterprises, Accellion offers clustering for multi-site load balancing, intelligent replication and failover.

Accellion is a privately held company headquartered in Palo Alto, California with offices in North America, Asia and Europe.

www.accellion.com **info@accellion.com**